学校编码：10384　　分类号_____密级 _____

学号：X2006221027　　UDC _____

厦门大学

工　程　硕　士　学　位　论　文

基于 802.1x 协议校园网 ARP 欺骗主动防御系统的研究与实现

802.1x protocol-based ARP spoofing Active Defense System in campus network

薛　芳

指导教师姓名：　吴　锦　林　教授

专　业　名　称：　计　算　机　技　术

论文提交日期：　2011　年　4　月

论文答辩日期：　2011　年　　月

学位授予日期：　2011　年　　月

答辩委员会主席：_____

评　　阅　　人：_____

2011 年 4 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　√　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘 要

ARP 协议负责实现 IP 地址到网络接口硬件地址的映射，是 TCP/IP 协议族中最重要协议之一，但在设计之初并没有过多考虑安全问题，从而导致网络上出现了很多利用 ARP 协议进行黑客攻击的行为。自从 2006 年 ARP 欺骗病毒爆发，到现在仍不断出现新型 ARP 欺骗病毒，造成大面积用户无法上网或泄露敏感信息等危害，给校园网正常运行和安全带来极大的危害，使其成为影响校园网管理最大的一种安全威胁。

ARP 病毒对中毒机器的危害较小，主要是攻击网络中的其他主机，现有 ARP 欺骗攻击的防御手段主要是为了防止正常用户不受欺骗，无法对中毒机器进行处理，中了 ARP 欺骗木马的用户无法感知。所以最有效的办法还是迅速阻断这种攻击的来源，能够快速检测到攻击并定位出攻击主机位置后加以处理。本系统针对整个本校普遍存在的 ARP 欺骗攻击导致网络不稳定的情况，结合校园网实际网络特点，研究 ARP 欺骗攻击原理，通过分析三层交换机 ARP 表和镜像汇聚层端口数据方式捕获欺骗事件，实现了中毒计算机的自动定位。并基于已部署的 802.1x 认证系统定位 ARP 欺骗源，通过 SNMP 协议关闭进行 ARP 欺骗攻击的中毒主机端口，有效起到防御 ARP 欺骗攻击作用。

在校园网一个分区试运行一段时间内，该系统能有效地识别 ARP 欺骗事件，实现了欺骗源自动发现、自动处理，简化校园网络管理工作，大大减轻了网络管理员查找处理工作量，使校园网能正常稳定的运行，减少用户抱怨。

关键词：ARP 欺骗；802.1x；主动防御

ABSTRACT

ARP protocol is responsible for the completion of the mapping of IP addresses to network interface hardware address. As one of the fundamental protocols of the tcp/ip members, at the beginning of this agreement bunch of making, there is not much consideration to the secure questions. ARP protocol lack of effective authentication mechanism, we can not determine the authenticity of the data packet. At present, the network has already emerged on a lot of defects around the ARP protocol hacking behavior. Since 2006, ARP spoofing virus outbreak, and now continued emergence of new ARP spoofing virus, causing a large number the user can not access Internet or disclose sensitive information , these acts give the campus network security and the network management have had a great impact.

ARP spoofing viruses are less harmful to the poisoning machine , mainly to attack other hosts on the network , existing means of dealing with ARP spoofing are to prevent normal users from cheating , the poisoning users can not perceive . So the most effective way is to block the source of this attack, to quickly detect and locate the poisoning host .To deal with arp spoofing attacks resulted in network unstable situation , this paper combined the actual features of campus network , carried on the detailed analysis to arp spoofing attacks principle . By analyzing arp tables and mirroring data of the gateway , we can get the arp spoofing events . Based on the deployed 802. 1x certification system, close the port of the poisoning host by SNMP protocol , thus you can efectively performs to portect and detect this kind of attack.

The result shows that the system can effectively identify the ARP spoofing events, make the poisoning machine can be discovered and processed automatically . Simplify the management of campus networks, significantly reducing the workload of network administrators , so campus

network can be normal and stable operation, reducing user complaints.

Keywords: ARP proofing; 802.1x; Active defense

目录

Table of Contents

第一章 绪论

1.1 论文的研究背景

随着时代的发展，网络的日益普及，网络的使用已深入到各行各业，校园网为学校教学科研教育提供基础网络设施，并提供资源共享、信息交流和协同工作的计算机网络信息系统,已成为高校教育的重要组成部分。高校校园网络规模大、网络环境开放、各种计算机系统管理复杂、用户群体活跃而不安定，随之而来的网络安全问题也日渐明显地摆在了校园网络管理员面前。

计算机技术被迅速掌握的同时，出现了大批以病毒盈利的程序开发者。如今，计算机病毒变得更加活跃，木马、蠕虫、后门等病毒轮番攻击互联网。2000 年以来，由于病毒的基本技术和原理被越来越多的人所掌握，新病毒的出现以及原有病毒的变种层出不穷，病毒的增长速度也远远超过的以往任何时期。根据最新的 07 年上半年病毒总结发现，仅上半年新增病毒就达 11 万种，其中以盗取用户信息为主的木马程序就占到了 7 成。

所有利用 ARP 协议缺陷的多种恶意程序都被称为 ARP 木马。ARP 是地址解析协议（Address Resolution Protocol），1982 年的 RFC826 中提出并沿用至今，解决了 IP 地址到 MAC 地址的转化问题，是 TCP/IP 协议族中最重要协议之一，但在设计之初并没有过多考虑安全问题，使得 ARP 协议缺乏有效的认证机制，无法判断接受的数据包内数据的真实性，从而导致问题的产生。ARP 欺骗具有隐蔽性、随机性的特点，在 Internet 上随处可下载的 ARP 欺骗工具使 ARP 欺骗更加普遍。目前利用 ARP 欺骗的木马病毒在局域网中广泛传播,给网络安全运行带来巨大隐患，是局域网安全的首要威胁，自从 2006 年 ARP 欺骗病毒爆发，到现在仍不断出现新型 ARP 欺骗病毒，造成大面积用户无法上网或泄露敏感信息等危害，由于 ARP 欺骗利用 TCP/IP 协议缺陷，造成长时间没有一个彻底的解决方案，给校园网正常运行和安全带来极大的危害，使其成为影响校园网管理最大的一种安全威胁。

ARP 病毒对中毒机器的危害较小，其主要是攻击网络中的其他主机，现有

对 ARP 欺骗攻击的防御手段主要是为了防止正常用户不受欺骗，无法对中毒机器进行处理，中了 ARP 欺骗木马的用户无法感知。所以当前最有效的办法还是迅速阻断这种攻击的来源。这就要求能够快速检测到攻击并定位出攻击主机位置后加以处理。

1.2 国内外研究现状

ARP 木马防范的困难在于无法阻止问题的产生，因为其利用的是 ARP 协议自身设计中无法进行真实性验证的漏洞，不像软件的漏洞可以通过打补丁消除，也无法使已有的操作系统抛弃现在使用的协议改用修改后的协议；此外，现有监控技术主要针对主干网，而 ARP 木马只在局域网内起作用，网络中心难以在第一时间监测检测到局域网内的问题的发生，而接入层设备通常为二层设备，不能提供足够的控制功能。

目前主要的防范措施有以下几种：

通过客户端程序在用户主机上保证网关 IP-MAC 对应的真实性，在网关上通过 IP-MAC 绑定来保证网内主机 IP-MAC 的真实性，通过这两种方式可以一定程度上进行真实性验证，从而使 ARP 木马的危害得到控制。此类解决方案优点是：简单、小规模网络内易实施、见效快。缺点是：大规模网络不易部署、影响网络的移动性（用户换一个网段就必须重新确认绑定）、治标不治本，网络内的攻击机仍然在发送大量的欺骗数据包，严重浪费网络带宽，网络性能仍然没有得到有效改善。因此，必须查到“元凶”，阻止其向网络内发送欺骗数据包，净化网络流量。

在局域网内架设 ARP 服务器，替代主机应答 ARP 包。但其配置复杂，需要改变客户端设置。成本高，需要大量的服务器。

下载和使用防 ARP 攻击的软件，如 AntiARP 等。需要用户端都安装才能防止欺骗，并且无法保证网关不被欺骗。

开启交换机上针对 ARP 欺骗的特定功能。由于 ARP 欺骗攻击严重影响了网络的正常运行,各交换机厂家也积极应对 ARP 欺骗攻击的特点提供了相应的解决策略。如在锐捷 S21 系列二层交换机上可以通过开启 Anti - ARP - Spoofing 功能,防止同一网段内针对用户的 ARP 欺骗攻击。CISCO 的可以使用 ARP -

Inspection ， H3C 的可以使用 Anti- ARP - atttack 。由于我校校园网是分期建设，存在各厂商设备，配置复杂，且由于建设经费问题还有不少旧的接入设备无此功能。

网络用户计算机运用水平和安全意识参差不齐，想要从源头杜绝 ARP 欺骗还是不太现实。到目前为止，仅由网络管理员通过技术措施来完全杜绝 ARP 欺骗，也是无法做到的。

1.3 研究内容和组织结构

本系统针对整个教育网普遍存在的 ARP 欺骗攻击导致网络不稳定的情况，结合本校实际网络特点，研究 ARP 欺骗攻击的判别方法，并基于本校的 802.1x 认证系统设计一套管理软件，实现对 ARP 欺骗攻击事件自动发现、追踪欺骗源并自动处理等功能。

在对 ARP 协议和 802.1x 协议的研究分析的基础上，实现本系统的设计目标，设计系统的整体结构，并对系统各个模块进行分析和设计。完成系统各个模块功能的实现并进行区域测试。

本文主要包括三个部分：

第一部分由第二、三章组成，主要介绍了 ARP 协议的工作原理、ARP 欺骗攻击的原理和研究分析 IEEE 802.1x 协议认证系统的体系结构及认证机制与流程。

第二部分包括第四章到第七章，介绍了该系统总体设计和各主要模块的具体实现。

第三部分由第八、九章构成，主要讨论了系统的测试情况和应用效果，并对论文工作做了总结和展望。

第二章 ARP 协议分析

2.1 ARP 协议分析

ARP，全称 Address Resolution Protocol，中文名为地址解析协议，它工作在数据链路层，在本层和硬件接口联系，同时对上层提供服务。

二层的以太网交换设备不能识别 32 位的 IP 地址，它们是以 48 位以太网地址（MAC 地址）传输以太网数据包的，因此 IP 地址与 MAC 地址之间就必须存在一种对应关系，而 ARP 协议就是用来确定这种对应关系的协议。

在以太网中传输的数据包是以太包，而以太包是依据其首部的 MAC 地址来进行寻址的。发送方必须知道目的主机的 MAC 地址才能向其发送数据。ARP 协议的作用就在于把逻辑地址转换成物理地址，也即是把 32 位的 IP 地址变换成 48 位的以太网地址。为避免频繁发送 ARP 包进行寻址，每台主机或设备都有一个 ARP 高速缓存，其中记录了最近一段时间内其它 IP 地址与其 MAC 地址的对应关系。

2.1.1 ARP 的工作原理

ARP 的工作原理如下：

1、 首先，每台主机都会在自己的 ARP 缓存区 （ARP Cache）中建立一个 ARP 列表，以表示 IP 地址和 MAC 地址的对应关系。

2、 当源主机需要将一个数据包要发送到目的主机时，会首先检查自己 ARP 列表中是否存在目的主机 IP 地址对应的 MAC 地址，如果有，就直接将数据包发送到这个 MAC 地址；如果没有，就向本地网段发起一个 ARP 请求的广播包，查询此目的主机对应的 MAC 地址。此 ARP 请求数据包里包括源主机的 IP 地址、硬件地址、以及目的主机的 IP 地址。

3、 网络中所有的主机收到这个 ARP 请求后，会检查数据包中的目的 IP 是否和自己的 IP 地址一致。如果不相同就忽略此数据包；如果相同，该主机首先将发送端的 MAC 地址和 IP 地址添加到自己的 ARP 缓存中，如果 ARP 表中已经存在该 IP 的信息，则将其更新，然后给源主机发送一个 ARP 响应数据包，告诉

对方自己是它需要查找的 MAC 地址；

4、 源主机收到这个 ARP 响应数据包后，将得到的目的主机的 IP 地址和 MAC 地址添加到自己的 ARP 缓存中，并利用此信息开始数据的传输。如果源主机一直没有收到 ARP 响应数据包，表示 ARP 查询失败。

2.1.2 ARP 报头结构

<table>
<tr><td colspan="2">硬件类型</td><td>协议类型</td></tr>
<tr><td>硬件地址长度</td><td>协议长度</td><td>操作类型</td></tr>
<tr><td colspan="3">源物理地址（0-3 字节）</td></tr>
<tr><td colspan="2">源物理地址（4-5 字节）</td><td>源 IP 地址（0-1 字节）</td></tr>
<tr><td colspan="2">源 IP 地址（2-3 字节）</td><td>目标硬件地址（0-1 字节）</td></tr>
<tr><td colspan="3">目标硬件地址（2-5 字节）</td></tr>
<tr><td colspan="3">目标 IP 地址（0-3 字节）</td></tr>
</table>

图 2.1:ARP 报头结构

- 硬件类型字段：表明 ARP 实现在何种类型的网络上，以太网的值为 1；
- 协议类型字段：发送方提供的高层协议类型，IP 为 0800H；
- 硬件地址长度和协议长度：硬件地址和高层协议地址的长度，这样 ARP 报文就可以在任意硬件和任意协议的网络中使用；
- 操作类型：表示这个报文的类型，ARP 请求为 1，ARP 响应为 2，RARP 请求为 3，RARP 响应为 4；
- 源物理地址：源主机硬件地址；
- 源 IP 地址：源主机硬件地址；
- 目标硬件地址：目的主机硬件地址；
- 目的 IP 地址：目的主机的 IP 地址。

2.2 ARP 欺骗原理

以太局域网内数据包传输依靠的是 MAC 地址，IP 地址与 MAC 对应的关系依

靠 ARP 缓存表，每台主机（包括网关）都有一个 ARP 缓存表。在正常情况下这个缓存表能够有效的保证数据传输的一对一性。但是在 ARP 缓存区的实现机制中存在一个不完善的地方，按照 ARP 协议的设计，为了减少网络上过多的 ARP 数据通信，一个主机，即使收到的 ARP 应答并非自己请求得到的，它也会将其插入到自己的 ARP 缓存区中或直接将应答包里的MAC地址与IP对应的关系替换掉原有的 ARP 缓存区里的相应信息。

以下是造成 ARP 欺骗的根本原因：

1、ARP 请求是广播的，大家都能接收到，这使 ARP 病毒有了合适的入侵时机。

2、默认的 ARP 更新规则，凡是接收到应答包就更新 ARP 缓冲区。

3、ARP 的更新中没有认证信息，这使的接收到应答包的机器只要能够解析其中的字段，就能更新自己的 MAC 表。

2.3 ARP 欺骗病毒

ARP 欺骗病毒指所有利用 ARP 协议漏洞、包含有 ARP 欺骗功能进行拒绝服务攻击(DoS)或中间人攻击的病毒的总称，造成网络通信中断或数据被截取和窜改，严重影响网络的安全。

2.3.1 ARP 欺骗病毒危害

影响局域网正常运行——局域网内一旦有 ARP 的攻击存在，会欺骗局域网内所有主机和网关，让所有上网的流量必须经过 ARP 攻击者控制的主机。其他用户原来直接通过网关上网现在转由通过被控主机转发上网，由于被控主机性能和程序性能的影响，这种转发并不会非常流畅，因此就会导致用户上网的速度变慢。而由于 ARP 表存在老化机制，这就导致在某段时候主机能获得正确的网关 MAC 直到新的欺骗完成，这两种情况的交替过程中，主机显示的状况就是网络时断时续。

泄露用户敏感信息——个人隐私泄露、帐号被盗用等（如游戏帐号和密码、QQ 号和密码、网银帐号和密码等）。

非法控制——网络速度、网络访问行为受第三方非法控制。